The US-CERT Cyber Security Bulletin provides a summary of new and updated vulnerabilities, exploits, trends, and malicious code that have recently been openly reported. Information in the Cyber Security Bulletin is a compilation of open source and US-CERT vulnerability information. As such, the Cyber Security Bulletin includes information published by sources outside of US-CERT and *should **not** be considered the result of US-CERT analysis or as an official report of US-CERT*. Although this information does reflect open source reports, it is not an official description and should be used for informational purposes only. The intention of the Cyber Security Bulletin is to serve as a comprehensive directory of pertinent vulnerability reports, providing brief summaries and additional sources for further investigation.

Vulnerabilities

- Windows Operating Systems
  - StoreBot 2002 Standard Edition Arbitrary Code Execution
  - StoreBot 2005 Professional Edition SQL Injection
  - Alt-N MDaemon Denial of Service
  - ArGoSoft Mail Server Pro Information Disclosure
  - ArGoSoft Mail Server Pro Arbitrary Code Execution
  - ArGoSoft FTP Server Arbitrary Code Execution
  - Bttlxe Forum Cross-Site Scripting
  - iCal Cross-Site Scripting
  - Cactusoft Parodia Cross-Site Scripting
  - Cilem News SQL injection
  - MTS Professional Open Email Relay
  - Visnetic AntiVirus Plug-in for MailServer Privilege Elevation
  - DirectContact Directory Traversal
  - HP System Management Homepage Directory Traversal
  - Ipswitch WhatsUp Professional 2006 Denial Of Service
  - M4 Project enigma-suite Security Restriction Bypassing
  - Macromedia Shockwave Arbitrary Code Execution
  - Microsoft Internet Explorer Arbitrary Code Execution
  - Microsoft Word Denial of Service
  - NetworkActiv Web Server Information Disclosure
  - Winamp Arbitrary Code Execution
  - Pentacle In-Out Board SQL Injection or Security Restriction Bypassing
  - The Bat! Arbitrary Code Execution
  - Multiple SpeedProject Applications Remote Directory Traversal Vulnerability
  - Virtual Communication Services VPMi SQL Injection
  - WinACE Directory Traversal
  - WinACE Arbitrary Code Execution
- Unix/ Linux Operating Systems
  - CrossFire Remote Denial of Service
  - FreeBSD Remote NFS Mount Request Denial of Service
  - GNOME Evolution Remote Denial of Service
  - **GNU Tar PAX Remote Buffer Overflow (Updated)**
  - **GnuPG Detached Signature Verification Bypass (Updated)**
  - ViRobot Linux Server Authentication Bypass
  - **ImageMagick Utilities Image Filename Remote Command Execution (Updated)**
  - iUser Ecommerce File Inclusion
  - BMV Buffer Overflow (Updated)
  - Lincoln D. Stein Crypt::CBC Perl Module Weak Ciphertext Security Bypass
  - **Multiple Vendors Linux Kernel Integer Overflow (Updated)**
  - **Multiple Vendors Linux Kernel Find_Target Local Denial of Service (Updated)**
  - **Multiple Vendors Heimdal TelnetD Remote Denial of Service (Updated)**
  - **Multiple Vendors Sudo Python Environment Cleaning Security Bypass (Updated)**
  - **Multiple Vendors Linux Kernel Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Kernel NFS ACL Access Control Bypass (Updated)**
  - **Multiple Vendors Linux Kernel ProcFS Kernel Memory Disclosure (Updated)**
  - **Multiple Vendors Noweb Insecure Temporary File Creation (Updated)**
  - Multiple Vendors OpenSSH Remote Denial of Service
  - **Multiple Vendors Linux Kernel 'mq_open' System Call Denial of Service (Updated)**
  - Multiple Vendors Linux Kernel Denial of Service
  - **Multiple Vendors Perl 'miniserv.pl' script Format String (Updated)**
  - PHP PEAR::Archive_Tar Remote Directory Traversal
  - zoo Buffer Overflow
  - **Heimdal RSHD Server Elevated Privileges (Updated)**
  - **SCO UnixWare Ptrace Elevated Privileges (Updated)**
  - Sun Solaris HSFS Filesystem Denial of Service
  - SuSE YaST Online Update Script Signature Verification Bypass
- Multiple Operating Systems
  - 4images Remote File Include
  - **Apache mod_imap Cross-Site Scripting (Updated)**
  - Archangel Weblog Authentication Bypass
  - Brown Bear Software Calcium Cross-Site Scripting
  - CGI Calendar Cross-Site Scripting
  - Compex NetPassage WPE54G Denial of Service
  - CubeCart Arbitrary File Upload
  - ShoutLIVE Arbitrary PHP Code Execution & Cross-Site Scripting
  - D3Jeeb Multiple SQL Injection
  - DCI-Taskeen Multiple SQL Injection
  - DEV Web Management System HTML Injection
  - EJ3 TOPo Cross-Site Scripting
  - EKINboard Cross-Site Scripting & SQL Injection
  - **Ethereal OSPF Protocol Dissection Buffer Overflow (Updated)**
  - **Ethereal IRC & GTP Dissectors Remote Denial of Service (Updated)**
  - EZ Publish Cross-Site Scripting
  - Fantastic Scripts Fantastic News SQL Injection
  - **FortiGate URL Filter & Virus Scanning Bypass (Updated)**
  - PHP-Nuke SQL Injection

Vulnerabilities

The tables below summarize vulnerabilities that have been reported by various open source organizations or presented in newsgroups and on web sites. **Items in bold designate updates that have been made to past entries.** Entries are grouped by the operating system on which the reported software operates, and vulnerabilities which affect both Windows and Unix/ Linux Operating Systems are included in the Multiple Operating Systems table. *Note*, entries in each table are not necessarily vulnerabilities *in* that operating system, but vulnerabilities in software which operate on some version of that operating system.

Entries may contain additional US-CERT sponsored information, including Common Vulnerabilities and Exposures (CVE) numbers, National Vulnerability Database (NVD) links, Common Vulnerability Scoring System (CVSS) values, Open Vulnerability and Assessment Language (OVAL) definitions, or links to US-CERT Vulnerability Notes. Metrics, values, and information included in the Cyber Security Bulletin which has been provided by other US-CERT sponsored programs, is prepared, managed, and contributed by those respective programs. CVSS values are managed and provided by the US-CERT/ NIST National Vulnerability Database. Links are also provided to patches and workarounds that have been provided by the product's vendor.

The Risk levels are defined below:

High - Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

Medium - Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.

Low - Vulnerabilities will be labeled "Low" severity if they have a CVSS base score of 0.0-3.9.

Note that scores provided prior to 11/9/2005 are approximated from only partially available CVSS metric data. Such scores are marked as "Approximated" within NVD. In particular, the following CVSS metrics are only partially available for these vulnerabilities and NVD assumes certain values based on an approximation algorithm: AccessComplexity, Authentication, ConfImpact of 'partial', IntegImpact of 'partial', AvailImpact of 'partial', and the impact biases.

Windows Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
Addsoft Corp StoreBot 2002 Standard Edition	A vulnerability has been reported in StoreBot 2002 Standard Edition that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing.	StoreBot 2002 Standard Edition Arbitrary Code Execution	Not available	Secunia, Advisory: SA19060, March 1, 2006

	A Proof of Concept exploit has been published.			
Addsoft Corp StoreBot 2005 Professional Edition	A vulnerability has been reported in StoreBot 2005 Professional Edition that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	StoreBot 2005 Professional Edition SQL Injection	Not available	Secunia, Advisory: SA19019, March 1, 2006
Alt-N MDaemon 8.1.1	A vulnerability has been reported in MDaemon, IMAP server, that could let remote malicious users cause a Denial of Service. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Alt-N MDaemon Denial of Service CVE-2006-0925	2.3	Security Focus, ID: 16854, February 27, 2006
ArGoSoft Mail Server Pro 1.8.8.1	A vulnerability has been reported in Mail Server Pro that could let remote malicious users disclose information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	ArGoSoft Mail Server Pro Information Disclosure CVE-2006-0928	2.3	Security Focus, ID: 16808, February 24, 2006
ArGoSoft Mail Server Pro 1.8.8.5 and prior	Multiple vulnerabilities have been reported in Mail Server Pro that could let remote malicious users to execute arbitrary code. ArGoSoft Mail Server Pro 1.8.8.6 There is no exploit code required.	ArGoSoft Mail Server Pro Arbitrary Code Execution	Not available	Security Focus, ID: 16834, February 27, 2006
ArGoSoft FTP Server 1.4.3.5 and prior	A buffer overflow vulnerability has been reported in ArGoSoft FTP Server that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	ArGoSoft FTP Server Arbitrary Code Execution	Not available	Security Tracker, Alert ID: 1015681, February 25, 2006
Battleaxe Software Bttlxe Forum 2.0	A vulnerability has been reported in Bttlxe Forum that could let remote malicious users conduct Cross-Site Scripting No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Bttlxe Forum Cross-Site Scripting	Not available	Security Focus, ID: 16821, February 25, 2006
Brown Bear Software iCal 3.10	A vulnerability has been reported in iCal that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	iCal Cross-Site Scripting CVE-2006-0924	4.7	Secunia, Advisory: SA19001, February 24, 2006
Cactusoft Parodia 6.2	A vulnerability has been reported in Parodia that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Cactusoft Parodia Cross-Site Scripting	Not available	Security Focus, ID: 16865, February 28, 2006
Cilem News 1.0, 1.1	A vulnerability has been reported in Cilem News that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Cilem News SQL injection	Not available	Security Focus, ID: 16813, February 24, 2006

Craig Morrison MTS Professional	A vulnerability has been reported in MTS Professional that could let remote malicious users utilize open email relay. No workaround or patch available at time of publishing. There is no exploit code required.	MTS Professional Open Email Relay	Not available	Security Focus, ID: 16840, February 27, 2006
Deerfield Visnetic AntiVirus Plug-in for MailServer 4.6.0.4, 4.6.1.1	A vulnerability has been reported in Visnetic AntiVirus Plug-in for MailServer that could let local malicious users obtain elevated privileges. Deerfield Visnetic AntiVirus 4.6.1.2 There is no exploit code required.	Visnetic AntiVirus Plug-in for MailServer Privilege Elevation CVE-2006-0812	7	Secunia, Advisory: SA16583, February 23, 2006
DirectContact 0.3b	A vulnerability has been reported in DirectContact that could let remote malicious users perform directory traversal. No workaround or patch available at time of publishing A Proof of Concept exploit has been published.	DirectContact Directory Traversal	Not available	Security Tracker, Alert ID: 1015686, February 27, 2006
HP System Management Homepage 2.0 through 2.0.1, 2.1 through 2.1.4	A vulnerability has been reported in System Management Homepage that could let remote malicious users perform directory traversal. HP Workaround Currently we are not aware of any exploits for this vulnerability.	HP System Management Homepage Directory Traversal	Not available	Security Tracker, Alert ID: 1015692, February 28, 2006
Ipswitch WhatsUp Professional 2006	A vulnerability has been reported in WhatsUp Professional 2006 that could let remote malicious users cause a Denial of Service. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Ipswitch WhatsUp Professional 2006 Denial Of Service CVE-2006-0911	2.3	Security Focus, ID: 16771, February 22, 2006
M4 Project enigma-suite 0.73.3	A vulnerability has been reported in M4 Project enigma-suite that could let remote malicious users bypass security restrictions. M4 Project enigma-suite Solution There is no exploit code required.	M4 Project enigma-suite Security Restriction Bypassing	Not available	Secunia, Advisory: SA19077, March 1, 2006
Macromedia Shockwave 10.1.0.11 & prior	A buffer overflow vulnerability has been reported when a particular ActiveX control is passed with malicious parameters, which could let a remote malicious user execute arbitrary code. This issue has been addressed by Adobe. Reportedly, no action needs to be taken by users to correct this vulnerability. Currently we are not aware of any exploits for this vulnerability.	Macromedia Shockwave Arbitrary Code Execution CVE-2005-3525	7	Security Focus, Bugtraq ID: 16791, February 23, 2006 US-CERT VU#437212
Microsoft Internet Explorer 6.0	A buffer overflow vulnerability has been reported in Internet Explorer that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. An exploit script, ie_iscomponentinstalled.pm, has been published.	Microsoft Internet Explorer Arbitrary Code Execution	Not available	Security Focus, ID: 16870, February 28, 2006
Microsoft Word	A vulnerability has been reported in Word that could let remote malicious users cause a Denial of Service. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Microsoft Word Denial of Service CVE-2006-0935	2.3	Security Focus, ID: 16782, February 23, 2006
NetworkActiv Web Server 3.5.15	A vulnerability has been reported in Web Server that could let remote malicious users disclose information. NetworkActiv Web Server 3.5.16	NetworkActiv Web Server Information Disclosure CVE-2006-0815	Not available	Secunia, Advisory: SA18947, March 1, 2006

	Currently we are not aware of any exploits for this vulnerability.			
Nullsoft Winamp 5.2 and prior	A buffer overflow vulnerability has been reported in Winamp that could let remote malicious users execute arbitrary code. Update to newest version of Winamp 5.2 There is no exploit code required.	Winamp Arbitrary Code Execution CVE-2006-0720	3.9	Security Tracker, Alert ID: 1015675, February 24, 2006
Pentacle In-Out Board 6.03	An input validation vulnerability has been reported in Pentacle In-Out Board that could let remote malicious users perform SQL injection or bypass security restrictions. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Pentacle In-Out Board SQL Injection or Security Restriction Bypassing	Not available	Security Tracker, Alert ID: 1015682, February 25, 2006
RIT Labs The Bat! 3.60.07	A buffer overflow vulnerability has been reported in The Bat! that could let remote malicious users execute arbitrary code. RIT Labs The Bat! 3.71.03 Currently we are not aware of any exploits for this vulnerability.	The Bat! Arbitrary Code Execution CVE-2006-0918	7	Secunia, Advisory: SA18989, February 24, 2006
SpeedProjects ZipStar 5.1, Squeez 5.1, SpeedCommander 11.0 build 4450	An input validation vulnerability has been reported in ZipStar, Squeez, and SpeedCommander that could let remote malicious users perform directory traversal. No workaround or patch available at time of publishing. There is no exploit code required.	Multiple SpeedProject Applications Remote Directory Traversal Vulnerability CVE-2006-0890	2.3	Secunia Advisory: SA19006, February 24, 2006
Virtual Communication Services VPMi 3.3	A vulnerability has been reported in VPMi that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Virtual Communication Services VPMi SQL Injection CVE-2006-0897	7	Security Focus, ID: 16798, February 24, 2006
WinACE 2.5, 2.6	An input validation vulnerability has been reported in WinACE, 'rar' and 'tar' handling, that could let remote malicious users perform directory traversal. No workaround or patch available at time of publishing. There is no exploit code required.	WinACE Directory Traversal	Not available	Security Focus, ID: 16800, February 24, 2006
WinACE 2.60	A buffer overflow vulnerability has been reported in WinACE, ARJ archive handling, that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	WinACE Arbitrary Code Execution CVE-2006-0813	3.9	Secunia, Advisory: SA17251, February 23, 2006

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
CrossFire CrossFire 1.8.0 & prior	A remote Denial of Service vulnerability has been reported in the 'oldsocketmode' option due to an error. Updates available There is no exploit code required.	CrossFire Remote Denial of Service CVE-2006-0677	3.3	Secunia Advisory: SA19044, February 28, 2006

FreeBSD FreeBSD 6.0 -STABLE, 6.0 -RELEASE	A remote Denial of Service vulnerability has been reported when handling NFS mount requests due to an error. Patches available A Proof of Concept exploit has been published.	FreeBSD Remote NFS Mount Request Denial of Service CVE-2006-0900	3.3	Secunia Advisory: SA19017, February 27, 2006
GNOME Development Team Evolution 2.3.1-2.3.7, 2.2.1, 2.2, 2.1, 2.0.1, 2.0, 1.5	A remote Denial of Service vulnerability has been reported. No workaround or patch available at time of publishing. A Proof of Concept exploit has been reported	GNOME Evolution Remote Denial of Service CVE-2006-0040	Not available	Security Focus, Bugtraq ID: 16899, March 1, 2006
GNU tar 1.15.90, 1.15.1, 1.14.90, 1.15, 1.14	A buffer overflow vulnerability has been reported when handling PAX extended headers due to a boundary error, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. GNU Mandriva Ubuntu **Trustix** Currently we are not aware of any exploits for this vulnerability.	GNU Tar PAX Remote Buffer Overflow CVE-2006-0300	**3.9**	Secunia Advisory: SA18973, February 22, 2006 Mandriva Security Advisory, MDKSA-2006:046, February 21, 2006 Ubuntu Security Notice, USN-257-1, February 23, 2006 **Trustix Secure Linux Security Advisory, #2006-0010, February 24, 2006**
GnuPG GnuPG / gpg prior to 1.4.2.1	A vulnerability has been reported because 'gpgv' exits with a return code of 0 even if the detached signature file did not carry any signature (if 'gpgv" or "gpg --verify' is used), which could let a remote malicious user bypass security restrictions. Patches available Fedora Debian Mandriva Ubuntu Gentoo SuSE **SuSE** There is no exploit code required; however, a Proof of Concept exploit has been published.	GnuPG Detached Signature Verification Bypass CVE-2006-0455	4.9	GnuPG Advisory, February 15, 2006 Fedora Update Notification, FEDORA-2006-116, February 17, 2006 Debian Security Advisory, DSA-978-1, February 17, 2006 Mandriva Security Advisory, MDKSA-2006:043, February 17, 2006 Ubuntu Security Notice, USN-252-1, February 17, 2006 Gentoo Linux Security Advisory, GLSA 200602-10, February 18, 2006 SuSE Security Announcement, SUSE-SA:2006:009, February 20, 2006 **SUSE Security Announcement, SUSE-SA:2006:013, March 1, 2006**
Hauri ViRobot Linux Server 2.0 20050817	A vulnerability has been reported in the 'filescan' CGI program due to insufficient credential validation when submitted via cookies, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required.	ViRobot Linux Server Authentication Bypass CVE-2006-0864	10	INetCop Security Advisory #2006-0x82-028, February 22, 2006
Image Magick ImageMagick 6.2.4.5	A vulnerability has been reported in the delegate code that is used by various ImageMagick utilities when handling an image filename due to an error, which	ImageMagick Utilities Image Filename Remote	7 (CVE-2005-4601)	Secunia Advisory: SA18261, December 30, 2005

	could let a remote malicious user execute arbitrary commands; and a format string vulnerability has been reported when handling filenames received via command line arguments, which could let a remote malicious user execute arbitrary code. Ubuntu Debian Mandriva Gentoo RedHat **Gentoo** There is no exploit code required.	Command Execution CVE-2005-4601 CVE-2006-0082	3.9 (CVE-2006-0082)	Ubuntu Security Notice, USN-246-1, January 24, 2006 Debian Security Advisory, DSA-957-1, January 26, 2006 Mandriva Security Advisory, MDKSA-2006:024, January 26, 2006 Gentoo Linux Security Advisory, GLSA 200602-06, February 13, 2006 RedHat Security Advisory, RHSA-2006:0178-4, February 14, 2006 **Gentoo Linux Security Advisory, GLSA 200602-13, February 26, 2006**
Intensive point iUser Ecommerce 2.1	A vulnerability has been reported in 'common.php' due to insufficient verification of the 'include_path' parameter before using to include files, which could let a remote malicious user include arbitrary files. Update available Currently we are not aware of any exploits for this vulnerability.	iUser Ecommerce File Inclusion CVE-2006-0854	7	Secunia Advisory: SA18903, February 23, 2006
Jan Kybic BMV 1.2	A buffer overflow vulnerability has been reported in the 'openpsfile()' function in 'gsinterf.c' due to an integer overflow error when allocating memory to store the file offsets of each page in a PS file, which could let a malicious user execute arbitrary code. **Debian** Currently we are not aware of any exploits for this vulnerability.	BMV Buffer Overflow CVE-2005-3278	7	Security Tracker Alert ID: 1015086, October 20, 2005 **Debian Security Advisory DSA-981-1, February 26, 2006**
Lincoln D. Stein Crypt::CBC 2.16 & prior	A vulnerability has been reported due to a flaw in its creation of IVs (Initialization Vectors) for ciphers with a blocksize larger than 8 when the RandonIV-style header is used, which could let a remote malicious user bypass security restrictions. Updates available Currently we are not aware of any exploits for this vulnerability.	Lincoln D. Stein Crypt::CBC Perl Module Weak Ciphertext Security Bypass CVE-2006-0898	1.3	Secunia Advisory: SA18755, February 27, 2006
Multiple Vendors Linux kernel 2.6-2.6.15	An integer overflow vulnerability has been reported in 'INVALIDATE_ INODE_PAGES2' which could lead to a Denial of Service and possibly execution of arbitrary code. Fedora Mandriva SuSE **SuSE** A Proof of Concept exploit script has been published.	Linux Kernel Integer Overflow CVE-2005-3808	3.5	Fedora Update Notification, FEDORA-2005-1138, December 13, 2005 Mandriva Security Advisory, MDKSA-2006:018, January 20, 2006 SUSE Security Announcement, SUSE-SA:2006:006, February 9, 2006 **SUSE Security Announcement, SUSE-SA:2006:012, February 27, 2006**

Multiple Vendors RedHat Enterprise Linux WS 3, ES 3, AS 3, Desktop 3.0; Linux kernel 2.4-2.4.28	A Denial of Service vulnerability has been reported in the 'find_target' function due to a failure to properly handle unexpected conditions when attempting to handle a NULL return value from another function. Upgrades available RedHat Debian Mandriva **SuSE** There is no exploit code required.	Linux Kernel Find_Target Local Denial of Service CVE-2005-2553	2.3	Security Focus, Bugtraq ID: 14965, September 28, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 Debian Security Advisory. DSA 921-1, December 14, 2005 Mandriva Security Advisory, MDKSA-2006:044, February 21, 2006 **SUSE Security Announcement, SUSE-SA:2006:012, February 27, 2006**
Multiple Vendors Royal Institute of Technology Heimdal 0.7, 0.6- 0.6.5, 0.5.0-0.5.3, 0.4 a-f; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha; Ubuntu Ubuntu Linux 5.10 powerpc Ubuntu Ubuntu Linux 5.10 i386 Ubuntu Ubuntu Linux 5.10 amd64 Ubuntu Linux 5.0 4 powerpc, i386, amd6, 4.1 ppc, ia64, ia32	A remote Denial of Service vulnerability has been reported in 'telnetd' due to a NULL pointer dereference error. Update to version 0.7.2 or 0.6.6. Debian Ubuntu **SuSE** There is no exploit code required.	Heimdal TelnetD Remote Denial of Service CVE-2006-0677	3.3	Bugtraq ID: 16676, February 16, 2006 Debian Security Advisory, DSA-977-1, February 16, 2006 Ubuntu Security Notice, USN-253-1, February 17, 2006 **SUSE Security Announcement, SUSE-SA:2006:011, February 24, 2006**
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Todd Miller Sudo 1.6-1.6.8, 1.5.6-1.5.9	A vulnerability has been reported in the 'PYTHONINSPECT' variable, which could let a malicious user bypass security restrictions and obtain elevated privileges. Todd Miller Sudo AppleWebSharing Update Conectiva Debian EnGarde Fedora FreeBSD GratiSoft Sudo Mandriva OpenPKG OpenBSD RedHat Slackware SuSE Trustix TurboLinux Ubuntu Wirex Debian SuSE Slackware **Trustix** An exploit script, sudo_local_python_	Sudo Python Environment Cleaning Security Bypass CVE-2006-0151	7	Security Focus, Bugtraq ID: 16184, January 9, 2006 Security Focus, Bugtraq ID: 16184, January 12, 2006 Debian Security Advisory, DSA-946-1, January 20, 2006 SUSE Security Summary Report, SUSE-SR:2006:002, January 20, 2006 Slackware Security Advisory, SSA:2006-045-08, February 14, 2006 Slackware Security Advisory, SSA:2006-045-08, February 14, 2006 **Trustix Secure Linux Security Advisory, #2006-0010, February 24, 2006**

	exploit.txt, has been published.			
Multiple Vendors Linux kernel 2.6-2.6.14	Multiple vulnerabilities have been reported: a Denial of Service vulnerability was reported in 'mm/mempolicy.c' when handling the policy system call; a remote Denial of Service vulnerability was reported in 'net/ipv4/fib_ frontend.c' when validating the header and payload of fib_lookup netlink messages; an off-by-one buffer overflow vulnerability was reported in 'kernel/sysctl.c,' which could let a malicious user cause a Denial of Service and potentially execute arbitrary code; and a buffer overflow vulnerability was reported in the DVB (Digital Video Broadcasting) driver subsystem, which could let a malicious user cause a Denial of Service or potentially execute arbitrary code. Updates available SuSE **SuSE** An exploit script has been published.	Linux Kernel Multiple Vulnerabilities CVE-2005-4635 CVE-2005-3358	2.3 (CVE-2005-4635) 3.5 (CVE-2005-3358)	Secunia Advisory: SA18216, January 4, 2006 SUSE Security Announcement, SUSE-SA:2006:006, February 9, 2006 **SUSE Security Announcement, SUSE-SA:2006:012, February 27, 2006**
Multiple Vendors Linux kernel 2.6-2.6.14 .4; SuSE Linux Professional 10.0 OSS, 10.0, Linux Personal 10.0 OSS	A vulnerability has been reported in the NFS implementation due to insufficient validation of remote user privileges before setting ACLs, which could let a remote malicious user bypass access controls. Updates available SuSE **SuSE** There is no exploit code required.	Linux Kernel NFS ACL Access Control Bypass CVE-2005-3623	2.3	Security Focus, Bugtraq ID: 16570, February 9, 2006 SUSE Security Announcement, SUSE-SA:2006:006, February 9, 2006 **SUSE Security Announcement, SUSE-SA:2006:012, February 27, 2006**
Multiple Vendors Linux kernel prior to 2.6.15	A memory disclosure vulnerability has been reported in the 'ProcFS' kernel, which could let a malicious user obtain sensitive information. Update available Fedora RedHat Ubuntu SuSE **SuSE** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ProcFS Kernel Memory Disclosure CVE-2005-4605	1.6	Security Focus, Bugtraq ID: 16284, January 17, 2006 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006 Ubuntu Security Notice, USN-244-1, January 18, 2006 SUSE Security Announcement, SUSE-SA:2006:006, February 9, 2006 **SUSE Security Announcement, SUSE-SA:2006:012, February 27, 2006**
Multiple Vendors Norman Ramsey Noweb 2.9 a, 2.10 c; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user overwrite critical files. Debian Ubuntu **Gentoo** There is no exploit code required.	Noweb Insecure Temporary File Creation CVE-2005-3342	**1.3**	Debian Security Advisory, DSA-968-1, February 13, 2006 Ubuntu Security Notice, USN-254-1, February 21, 2006 **Gentoo Linux Security Advisory, GLSA 200602-14, February 26, 2006**

Multiple Vendors OpenBSD OpenSSH 3.8.1 p1; FreeBSD 5.4 -RELENG, -RELEASE, -PRERELEASE, 5.3 -STABLE, -RELENG, -RELEASE, 5.3, 5.4-STABLE	A remote Denial of Service vulnerability has been reported due to a design flaw when handling connections when configured to use the OpenPAM authentication system. OpenBSD Currently we are not aware of any exploits for this vulnerability.	OpenSSH Remote Denial of Service CVE-2006-0883	Not available	Security Focus, Bugtraq ID: 16892, March 1, 2006
Multiple Vendors RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; Linux kernel 2.6.9	A Denial of Service vulnerability has been reported in the 'mq_open' system call. RedHat Ubuntu SuSE **SuSE** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'mq_open' System Call Denial of Service CVE-2005-3356	1.6	Security Focus, Bugtraq ID: 16283, January 17, 2006 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006 Ubuntu Security Notice, USN-244-1, January 18, 2006 SUSE Security Announcement, SUSE-SA:2006:006, February 9, 2006 **SUSE Security Announcement, SUSE-SA:2006:012, February 27, 2006**
Multiple Vendors SuSE Linux Professional 9.3 x86_64, 9.3, Linux Personal 9.3 x86_64, 9.3; Linux kernel 2.6.11-2.6.12 .5	A Denial of Service vulnerability has been reported in 'handle_stop_signal()' due to a race condition. Updates available SuSE There is no exploit code required.	Linux Kernel Denial of Service CVE-2005-3847	2.8	SUSE Security Announcement, SUSE-SA:2006:012, February 27, 2006

Multiple Vendors Webmin 0.88 -1.230, 0.85, 0.76-0.80, 0.51, 0.42, 0.41, 0.31, 0.22, 0.21, 0.8.5 Red Hat, 0.8.4, 0.8.3, 0.1-0.7; Usermin 1.160, 1.150, 1.140, 1.130, 1.120, 1.110, 1.0, 0.9-0.99, 0.4-0.8; Larry Wall Perl 5.8.3-5.8.7, 5.8.1, 5.8 .0-88.3, 5.8, 5.6.1, 5.6, 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03	A format string vulnerability has been reported in 'Perl_sv_vcatpvfnl' due to a failure to properly handle format specifiers in formatted printing functions, which could let a remote malicious user cause a Denial of Service. Webmin Fedora OpenPKG Mandriva Ubuntu Gentoo Gentoo Mandriva SUSE Trustix Ubuntu Fedora RedHat OpenBSD OpenBSD Debian **Sun** An exploit has been published.	Perl 'miniserv.pl' script Format String CVE-2005-3912 CVE-2005-3962	**7** (CVE-2005-3212) **4.9** (CVE-2005-3962)	Security Focus, Bugtraq ID: 15629, November 29, 2005 Fedora Update Notifications, FEDORA-2005-1113, 1116, & 1117, December 1 & 2, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.025, December 3, 2005 Mandriva Linux Security Advisory, MDKSA-2005:223, December 2, 2005 Ubuntu Security Notice, USN-222-1 December 02, 2005, December 2, 2005 Gentoo Linux Security Advisory, GLSA 200512-01 & 200512-02, December 7, 2005 US-CERT VU#948385 Mandriva Linux Security Advisory, MDKSA-2005:225, December 8, 2005 SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0070, December 9, 2005 Ubuntu Security Notice, USN-222-2, December 12, 2005 Fedora Update Notifications, FEDORA-2005-1144 & 1145, December 14, 2005 SUSE Security Summary Report, SUSE-SR:2005:030, December 16, 2005 RedHat Security Advisory, RHSA-2005:880-8, December 20, 2005 Security Focus, Bugtraq ID: 15629, January 4, 2006 Debian Security Advisory, DSA-943-1, January 16, 2006 **Sun(sm) Alert Notification Sun Alert ID: 102192, February 28, 2006**
PEAR PEAR::Archive_Zip 1.1, 1.2	A Directory Traversal vulnerability has been reported when extracting TAR files due to an input validation error, which could let a remote malicious user potentially execute arbitrary files and overwrite files. No workaround or patch available at time of publishing. Currently we are not aware of any	PHP PEAR::Archive_Tar Remote Directory Traversal CVE-2006-0931	2.3	Security Focus, Bugtraq ID: 16805, February 27, 2006

	exploits for this vulnerability.			
Rahul Dhesi Zoo 2.10	A buffer overflow vulnerability has been reported in the 'fullpath()' in 'misc.c' due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	zoo Buffer Overflow CVE-2006-0855	3.9	Security Tracker Alert ID: 1015668, February 23, 2006
Royal Institute of Technology Heimdal prior to 0.6.6 & 0.7.2	A vulnerability has been reported in the 'rshd' server when storing forwarded credentials due to an unspecified error, which could let a malicious user obtain elevated privileges. Update to version 0.7.2 or 0.6.6. Ubuntu Debian **SuSE** Currently we are not aware of any exploits for this vulnerability.	Heimdal RSHD Server Elevated Privileges CVE-2006-0582	1.6	Security Tracker Alert ID: 1015591, February 7, 2006 Ubuntu Security Notice, USN-247-1, February 09, 2006 Debian Security Advisory, DSA-977-1, February 16, 2006 **SUSE Security Announcement, SUSE-SA:2006:011, February 24, 2006**
SCO Unixware 7.1.4, 7.1.3	A vulnerability has been reported in the 'ptrace()' system call due to an unspecified error, which could let a malicious user obtain elevated privileges. Updates available **A Proof of Concept exploit script, sco-root-exploit.c, has been published.**	SCO UnixWare Ptrace Elevated Privileges CVE-2005-2934	**7**	SCO Security Advisory, SCOSA-2006.9, February 21, 2006 **Security Focus, Bugtraq ID: 16765, February 27, 2006**
Sun Microsystems, Inc. Solaris 10.0 _x86, 10.0, 9.0 _x86, 9.0, 8.0 _x86, 8.0	A Denial of Service vulnerability has been reported in the 'hsfs' module due to an unspecified error. Patches available There is no exploit code required.	Sun Solaris HSFS Filesystem Denial of Service CVE-2006-0901	7	Sun(sm) Alert Notification Sun Alert ID: 102161, February 24, 2006
SuSE UnitedLinux 1.0, Open-Enterprise-Server 1, Novell Linux Desktop 9.0, Linux Professional 10.0 OSS, 10.0, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 10.0 OSS, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Enterprise Server 9, 8, Linux Desktop 1.0	A vulnerability has been reported in SuSE YaST Online Update (YOU), which could let a remote malicious user bypass signature verification. Updates available There is no exploit code required.	SuSE YaST Online Update Script Signature Verification Bypass CVE-2006-0803	2.3	SUSE Security Announcement , SUSE-SA:2006:013, March 1, 2006

[back to top]

Multiple Operating Systems - Windows/UNIX/Linux/Other

Vendor & Software Name	Description	Common Name	CVSS	Resources
4images 4images 1.7.1 & prior	A file include vulnerability has been reported in 'index.php' due to insufficient verification of the 'template' parameter before using to include files, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, 4images_171_incl_xpl.php, has been published.	4images Remote File Include CVE-2006-0899	7	Secunia Advisory: SA19026, February 27, 2006

Apache Software Foundation Apache prior to 1.3.35-dev, 2.0.56-dev	A Cross-Site Scripting vulnerability has been reported in the 'Referer' directive in 'mod_imap' due to insufficient sanitization before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. The vulnerability has been fixed in version 1.3.35-dev, and 2.0.56-dev. OpenPKG Trustix Mandriva Ubuntu RedHat Fedora TurboLinux Gentoo **SuSE** There is no exploit code required.	Apache mod_imap Cross-Site Scripting CVE-2005-3352	2.3	Security Tracker Alert ID: 1015344, December 13, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.029, December 14, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0074, December 23, 2005 Mandriva Linux Security Advisory, MDKSA-2006:007, January 6, 2006 Ubuntu Security Notice, USN-241-1, January 12, 2006 RedHat Security Advisory, RHSA-2006:0158-4, January 17, 2006 Fedora Security Advisory, FEDORA-2006-052, January 23, 2006 Turbolinux Security Advisory, TLSA-2006-1, January 25, 2006 Gentoo Linux Security Advisory, GLSA 200602-03, February 6, 2006 **SUSE Security Summary Report, SUSE-SR:2006:004, February 24, 2006**
Archangel Management Archangel Weblog 0.90.02	A vulnerability has been reported due to insufficient validation of user-supplied data, which could let a remote malicious user bypass authentication. No workaround or patch available at time of publishing. Vulnerability can be exploited through use of a web client; however, a Proof of Concept exploit has been published.	Archangel Weblog Authentication Bypass CVE-2006-0944	7	Security Focus, Bugtraq ID: 16848, February 27, 2006
Brown Bear Software Calcium 3.10.1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'EventText' parameter when adding a new event, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through use of a web client.	Calcium Cross-Site Scripting CVE-2006-0889	2.3	Secunia Advisory: SA19007, February 27, 2006
CGI Calendar CGI Calendar 2.7, 2.8	A Cross-Site Scripting vulnerability has been reported in 'index.cgi' and 'viewday.cgi' due to insufficient sanitization of the 'year' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	CGI Calendar Cross-Site Scripting	Not available	Secunia Advisory: SA19066, February 28, 2006
Compex NetPassage WPE54G	A Denial of Service vulnerability has been reported in the 'uCongig' agent when handling certain UDP datagrams. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this	Compex NetPassage WPE54G Denial of Service	Not available	Security Tracker Alert ID: 1015690, February 28, 2006

	vulnerability.			
Cube Cart CubeCart 3.0.7 -pl1, 3.0.6, 3.0.4, 3.0.3	A file upload vulnerability has been reported in 'connector.php' due to insufficient authentication checks, which could let a remote malicious user execute arbitrary code. Updates available Vulnerability can be exploited with a web client.	CubeCart Arbitrary File Upload CVE-2006-0922	2.3	NSA Group Security Advisory NSAG-197-23.02.2006, February 21, 2006
Cynical Games ShoutLIVE 1.1.0	Several vulnerabilities have been reported: a vulnerability was reported in the 'savesettings.php' script due to insufficient access controls, which could let a remote malicious user execute arbitrary PHP code; and a Cross-Site Scripting vulnerability was reported in 'post.php' due to insufficient sanitization before saving, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	ShoutLIVE Arbitrary PHP Code Execution & Cross-Site Scripting CVE-2006-0940 CVE-2006-0941	7 (CVE-2006-0940) 2.3 (CVE-2006-0941)	Secunia Advisory: SA19047, February 27, 2006
D3Jeeb D3Jeeb Pro 3	SQL injection vulnerabilities have been reported in 'fastlinks.php' and 'catogary.php' due to insufficient sanitization of the 'catid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through use of a web client; however, a Proof of Concept exploit has been published.	D3Jeeb Multiple SQL Injection CVE-2006-0906	7	Secunia Advisory: SA19062, February 28, 2006
DCI-Designs DCI-Taskeen 1.03	Multiple SQL injection vulnerabilities have been reported in 'basket.php' and 'cat.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities may be exploited using a web client; however, a Proof of Concept exploit has been published.	DCI-Taskeen Multiple SQL Injection CVE-2006-0939	7	Security Tracker Alert ID: 1015685, February 25, 2006
Dev Dev Web Management System 1.5	An HTML vulnerability has been reported in the 'City/Region' field when registering for an account due to insufficient sanitization before using, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited using a web client.	DEV Web Management System HTML Injection CVE-2006-0886	2.3	Secunia Advisory: SA18714, February 24, 2006
EJ3 TOPo 2.2.178	A Cross-Site Scripting vulnerability has been reported in 'code/inc_header.php' due to insufficient sanitization of the 'gTopNombre' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through use of a web client; however, a Proof of Concept exploit has been published.	EJ3 TOPo Cross-Site Scripting	Not available	Secunia Advisory: SA19070, March 1, 2006
EKIN designs Ekinboard 1.0.3	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of [img] BBcode before converting to HTML, which could let a remote malicious user executed arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'config.php' due to insufficient sanitization of the '$_COOKIE['username']' and '$_COOKIE['password'] variables before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Patch instructions Vulnerabilities could be exploited with a web client.	EKINboard Cross-Site Scripting & SQL Injection	Not available	Secunia Advisory: SA19045, February 28, 2006

Ethereal Group Ethereal 0.10-0.10.13, 0.9-0.9.16, 0.8.19, 0.8.18, 0.8.13-0.8.15, 0.8.5, 0.8, 0.7.7	A buffer overflow vulnerability has been reported in the 'dissect_ospf_ v3_address_ prefix()' function in the OSPF protocol dissector due to a boundary error when converting received binary data to a human readable string, which could let a remote malicious user execute arbitrary code. Patch available Debian Gentoo Mandriva Fedora RedHat Avaya **SuSE** Currently we are not aware of any exploits for this vulnerability.	Ethereal OSPF Protocol Dissection Buffer Overflow CVE-2005-3651	7	iDefense Security Advisory, December 9, 2005 Debian Security Advisory DSA 920-1, December 13, 2005 Gentoo Linux Security Advisory, GLSA 200512-06, December 14, 2005 Mandriva Linux Security Advisory MDKSA-2005:227, December 15, 2005 Mandriva Linux Security Advisory MDKSA-2006:002, January 3, 2006 Fedora Update Notification FEDORA-2005-000, January 5, 2006 RedHat Security Advisory, RHSA-2006:0156-6, January 11, 2006 Avaya Security Advisory, ASA-2006-046, February 13, 2006 **SUSE Security Summary Report, SUSE-SR:2006:004, February 24, 2006**
Ethereal Group Ethereal 0.9.1-0.10.13.	A remote Denial of Service vulnerability has been reported in the IRC and GTP dissectors when a malicious user submits a specially crafted packet. Upgrades available Mandriva RedHat Avaya **SuSE** Currently we are not aware of any exploits for this vulnerability.	Ethereal IRC & GTP Dissectors Remote Denial of Service CVE-2005-4585	3.3	Ethereal Security Advisory, enpa-sa-00022, December 27, 2005 Mandriva Linux Security Advisory MDKSA-2006:002, January 3, 2006 RedHat Security Advisory, RHSA-2006:0156-6, January 11, 2006 Avaya Security Advisory, ASA-2006-046, February 13, 2006 **SUSE Security Summary Report, SUSE-SR:2006:004, February 24, 2006**
eZ systems eZ publish 3.7.3 & prior	A Cross-Site Scripting vulnerability has been reported in the 'ReferrerURL' parameter before displaying the input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	EZ Publish Cross-Site Scripting CVE-2006-0938	2.3	Security Tracker Alert ID: 1015683, February 25, 2006
Fantastic Scripts Fantastic News 2.1.1	An SQL injection vulnerability has been reported in 'news.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability may be exploited through a web browser; however, a Proof of Concept exploit has been published.	Fantastic Scripts Fantastic News SQL Injection	Not available	Security Focus, Bugtraq ID: 16842, February 27, 2006
Fortinet FortiOS 3.0 beta, 2.8 MR10	Several vulnerabilities have been reported: a vulnerability was reported because the URL blocking functionality can be bypassed, which could let a remote malicious user bypass antivirus protection; and	FortiGate URL Filter & Virus Scanning Bypass	7 (CVE-2005-3057) 7	Secunia Advisory: SA18844, February 13, 2006

	a vulnerability was reported because the virus scanning functionality can be bypassed when FTP files are sent under certain conditions. **Update information** There is no exploit code required; however, Proof of Concept exploit scripts, http_req.pl and Fortinet-url.txt, have been published.	CVE-2005-3057 CVE-2005-3058	(CVE-2005-3058)	**Fortinet Advisory, February 24, 2006**
Francisco Burzi PHP-Nuke 7.8 Patched 3.2	An SQL injection vulnerability has been reported in 'mainfile.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability may be exploited using a web client; however, a Proof of Concept exploit has been published.	PHP-Nuke SQL Injection CVE-2006-0907 CVE-2006-0908	7 (CVE-2006-0907) 7 (CVE-2006-0908)	waraxe-2006-SA#047, February 25, 2006
FreeHost Shop Website Generator 3.3	A vulnerability has been reported in 'process3.php' due to insufficient sanitization of the 'formname' parameter before using to create files, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability may be exploited using a web client; however, a Proof of Concept exploit has been published.	FreeHostShop Website Generator Arbitrary PHP Code Execution CVE-2006-0936	4.2	Security Focus, Bugtraq ID: 16823, February 25, 2006
iGENUS WebMail 2.0-2.0.2	A file include vulnerability has been reported in 'Config_Inc.php' due to insufficient verification of the 'SG_HOME' parameter before using to include files, which could let a remote malicious user execute arbitrary php code. No workaround or patch available at time of publishing. Vulnerability may be exploited using a web client; however, a Proof of Concept exploit scripts, igenus_xpl.pl and igenus_remote.txt, have been published.	iGenus WebMail File Include	Not available	Secunia Advisory: SA19036, February 27, 2006
JFacets JFacets 0.x	A vulnerability has been reported in the 'profileID' parameter in the URL because it is possible to change the profile, which could let a remote malicious user bypass security restrictions. Update available Currently we are not aware of any exploits for this vulnerability.	JFacets 'ProfileID' Security Restriction Bypass	Not available	Secunia Advisory: SA19031, February 28, 2006
JGS-XA Support JGS-Gallery 4.0	Multiple Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited using a web client; however, a Proof of Concept exploit has been published.	JGS-Gallery Module Multiple Cross-Site Scripting CVE-2006-0927	5.6	Security Focus, Bugtraq ID: 16810, February 27, 2006
Lewis Media Simple Machines SMF 1.0.6	An HTML injection vulnerability has been reported due to insufficient sanitization of the 'X-Forwarded-For' HTTP header, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability may be exploited through a web browser.	Simple Machines HTML Injection CVE-2006-0896	7	Secunia Advisory: SA19004, February 24, 2006
Miro Software Solutions Pty Ltd. Oi! Email Marketing 3.0	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of 'myname' parameters before using in a SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing.	Oi! Email Marketing System SQL Injection CVE-2006-0919	7	Secunia Advisory: SA18993, February 24, 2006

	Vulnerability can be exploited through a web client; however; a Proof of Concept exploit has been published.			
MitriDAT Limited Web Calendar Pro 0	An SQL injection vulnerability has been reported in 'dropbase.php' due to insufficient sanitization of the the 'tabls' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit URL has been published.	Web Calendar Pro SQL Injection CVE-2006-0835	7	Security Focus, Bugtraq ID: 16789, February 23, 2006
Mozilla.org Thunderbird 1.5	Multiple vulnerabilities have been reported due to insufficient restrictions for downloading remote content in email messages, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script, thunderbird_email.txt, has been reported.	Mozilla Thunderbird Multiple Remote Information Disclosure	Not available	Security Focus, Bugtraq ID: 16881, February 28, 2006
Multiple Vendors RunCMS 1.2, 1.1 A, 1.1, 1.3.a5, 1.3.a2, 1.3.a; phpRPC 0.7-0.9	A vulnerability has been reported in 'rpc_decoder.php' in the 'decode()' function when decoding received XML data, which could let a remote malicious user execute arbitrary php code. No workaround or patch available at time of publishing. Vulnerability may be exploited via a web browser.	PHPRPC Library Arbitrary PHP Code Execution	Not available	Security Focus, Bugtraq ID: 16833, February 27, 2006
MyBB Group MyBB 1.0.4	An SQL injection vulnerability has been reported in 'misc.php' via cookies due to insufficient sanitization of the 'comma' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	MyBB SQL Injection	Not available	Secunia Advisory: SA19061, March 1, 2006
myPHP Nuke myPHPNuke 1.8.8 & prior	Cross-Site Scripting vulnerabilities have been reported in 'reviews.php' due to insufficient sanitization of the 'letter' parameter and in 'download.php' due to insufficient sanitization of the 'dcategory' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	MyPHPNuke Cross-Site Scripting CVE-2006-0923	2.3	Secunia Advisory: SA19052, February 27, 2006
MySQL AB MySQL 5.0.18	A vulnerability has been reported when handling query logging due to a discrepancy between the handling of NULL bytes in input data, which could let a remote malicious user bypass certain security restrictions. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	MySQL Query Logging Bypass CVE-2006-0903	4.9	Security Focus, Bugtraq ID: 16850, February 27, 2006
Nathan Landry n8cms 1.2, 1.1	Several vulnerabilities have been reported: an SQL injection was reported in 'index.php' due to insufficient sanitization of the 'dir' and 'page_id' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in 'mailto.php' due to insufficient sanitization of the 'userid' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through use of a web	N8cms SQL Injection & Cross-Site Scripting	Not available	Secunia Advisory: SA19068, March 1, 2006

	client; however, Proof of Concept exploits have been published.			
NetGear WGT624 0	A vulnerability has been reported when configured to backup configuration settings because various information is stored in cleartext, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	Netgear WGT624 Wireless Firewall Router Information Disclosure	Not available	Security Focus, Bugtraq ID: 16837, February 27, 2006
NOCC NOCC 1.0	Multiple vulnerabilities have been reported: a file include vulnerability was reported in 'index.php' due to insufficient verification of the 'lang' and 'theme' parameters and the 'Accept-Language' HTTP header, which could let a remote malicious user include arbitrary files and execute arbitrary PHP code; a vulnerability was reported in the 'profiles' directory due to the insecure storage of user preferences, which could let a remote malicious user obtain sensitive information; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of unspecified input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'html/header.php' because a remote malicious user can obtain the full path by accessing it directly. No workaround or patch available at time of publishing. Vulnerabilities can be exploited using a web client and a Proof of Concept exploit script, noccw_10_incl_xpl.php, has been published.	NOCC Webmail Input Validation CVE-2006-0891 CVE-2006-0892 CVE-2006-0893 CVE-2006-0894 CVE-2006-0895	2.3 (CVE-2006-0891) 7 (CVE-2006-0892) 2.3 (CVE-2006-0893) 2.3 (CVE-2006-0894) 2.3 (CVE-2006-0895)	Security Focus, Bugtraq ID: 16793, February 23, 2006
NuFW NuFW prior to 1.0.21	A remote Denial of Service vulnerability has been reported when handling blocked TLS sockets due to an error. Updates available There is no exploit code required.	NuFW TLS Socket Remote Denial of Service	Not available	Secunia Advisory: SA19046, February 28, 2006
One-Network.Org Lansuite 2.1	An SQL injection vulnerability has been reported in the Board module due to insufficient sanitization of the 'fid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability may be exploited using a web client; however, a Proof of Concept exploit script, lansuite_sql_poc, has been published.	LanSuite SQL Injection	Not available	Secunia Advisory: SA19048, February 27, 2006
Oracle Diagnostics 2.0-2.2, Oracle Applications 11i 11.5.10 CU1 & CU2,11i 11i 11.5.3-11.5.10	Multiple vulnerabilities have been reported including insecure permissions vulnerabilities, access vulnerabilities, and SQL injection vulnerabilities, which could let a remote malicious user obtain sensitive information or execute arbitrary SQL code. Patch information Vulnerabilities would likely be exploited from a web browser; however, a Proof of Concept exploit has been published.	Oracle Diagnostics Multiple Vulnerabilities	Not available	Security Focus, Bugtraq ID: 16844, February 27, 2006
PEHEPE Membership Management System PEHEPE Membership Management System 3.0	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'sol_menu.php' due to insufficient sanitization of the 'kuladi' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'sol_menu.php' due to insufficient verification of the 'uye_klasor' parameter before using to include files, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through use of a web client; however, Proof of Concept exploits have been published.	PEHEPE Membership Management System Cross-Site Scripting & File Include	Not available	Secunia Advisory: SA19055, March 1, 2006

PHP Group PHP 4.x, 5.1.2	Multiple input validation vulnerabilities have been reported in the 'mb_send_mail()' function, the 'mail()' function, and various PHP IMAP functions, which could allow 'safe_mode' and 'open_basedir' security settings to be bypassed. No workaround or patch available at time of publishing. Vulnerabilities can be exploited with a Web browser; however, a Proof of Concept exploit has been published.	PHP Security Bypass	Not available	Security Focus, Bugtraq ID: 16878, February 28, 2006
PHP Group PHP prior to 5.1.2	A Cross-Site Scripting vulnerability has been reported in pages that are generated under certain error conditions due to insufficient filtering of HTML code from user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Updates available Currently we are not aware of any exploits for this vulnerability.	PHP Cross-Site Scripting	Not available	Security Tracker Alert ID: 1015694, February 28, 2006
PHP PHP 5.1.1, 5.1	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient of the session ID in the session extension before returning to the user, which could let a remote malicious user inject arbitrary HTTP headers; a format string vulnerability was reported in the 'mysqli' extension when processing error messages, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insufficient sanitization of unspecified input that is passed under certain error conditions, which could let a remote malicious user execute arbitrary HTML and script code. PHP Mandriva **SuSE** There is no exploit code required.	Multiple PHP CVE-2006-0678 CVE-2006-0208	1.9 (CVE-2006-0678) 2.3 (CVE-2006-0208)	Secunia Advisory: SA18431, January 13, 2006 Mandriva Security Advisory, MDKSA-2006:028, February 1, 2006 **SUSE Security Summary Report, SUSE-SR:2006:004, February 24, 2006**
php Website Development Team phpWebsite 0.10-0.10.2, 0.9.3-0.9.3 -4, 0.8.2, 0.8.3, 0.7.3	An SQL injection vulnerability has been reported in 'topics.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability may be exploited using a web client; however, a Proof of Concept exploit script, phpWebSite-topic-sql-inj.pl, has been published.	PHPWebSite SQL Injection	Not available	Security Focus, Bugtraq ID: 16825, February 25, 2006
PHPLib Team PHPLIB 7.4	A vulnerability has been reported due to an unspecified error, which could let a remote malicious user execute arbitrary PHP code. Update available Currently we are not aware of any exploits for this vulnerability.	PHPLIB Arbitrary PHP Code Execution CVE-2006-0887	7	Security Focus, Bugtraq ID: 16801, February 27, 2006
PHPX PHPX 3.5.9	An HTML injection vulnerability has been reported due to insufficient verification of the 'url' XCode tag when posting a message, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability may be exploited via a web browser; however, a Proof of Concept exploit has been published.	PHPX HTML Injection CVE-2006-0933	2.3	Secunia Advisory: SA18688, February 27, 2006
POPFile POPFile 0.22.3	A remote Denial of Service vulnerability has been reported due to an error when handling email messages that contain certain character sets. Update available There is no exploit code required.	POPFile Remote Denial of Service CVE-2006-0876	2.3	Secunia Advisory: SA18975, February 23, 2006

PostgreSQL PostgreSQL 8.1.2, 8.1.1, 8.1	Several vulnerabilities have been reported: a vulnerability was reported in the 'SET ROLE" command when previous role settings are restored after an error, which could let a malicious user obtain superuser privileges; and a Denial of Service vulnerability was reported due to an error in the 'SET SESSION AUTHORIZATION' command if compiled with 'Asserts' enabled. Updates available OpenPKG **Trustix** **Ubuntu** There is no exploit code required.	PostgreSQL Privilege Escalation & Denial of Service CVE-2006-0553 CVE-2006-0678	4.2 (CVE-2006-0553) 1.9 (CVE-2006-0678)	Secunia Advisory: SA18890, February 15, 2006 OpenPKG Security Advisory, OpenPKG-SA-2006.004, February 19, 2005 **Trustix Secure Linux Security Advisory, #2006-0008, February 17, 2006** **Ubuntu Security Notice, USN-258-1, February 27, 2006** **US-CERT VU#567452**
PunBB PunBB 1.2.10	A Cross-Site Scripting vulnerability has been reported in 'header.php' due to insufficient sanitization of the path name before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Update available Vulnerability can be exploited through use of a web client.	PunBB Cross-Site Scripting	Not available	Secunia Advisory: SA19039, March 1, 2006
PwsPHP PwsPHP 1.2.3	An SQL injection vulnerability has been reported in the 'sondage' module due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Patch available A Proof of Concept exploit has been published.	PwsPHP SQL Injection CVE-2006-0943	7 (CVE-2006-0943)	Secunia Advisory: SA19023, February 27, 2006
QwikiWiki QwikiWiki 1.4	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through use of a web client; however, a Proof of Concept exploit has been published.	QwikiWiki Cross-Site Scripting	Not available	Security Focus, Bugtraq ID: 16874, February 28, 2006
Smith Micro ZipMagic Deluxe 9.0; StuffIt Standard 9.0, StuffIt Expander 9.0, StuffIt Deluxe 9.0	A Directory Traversal vulnerability has been reported when extracting compressed archives (.tar and .zip) due to an input validation error, which could let a remote malicious user execute and overwrite arbitrary files. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	StuffIt & ZipMagic Remote Directory Traversal CVE-2006-0926	2.3	Security Focus, Bugtraq ID: 16806, February 27, 2006
SPiD SPiD 1.3.1	A file include vulnerability has been reported in 'scan_lang_insert.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary files. No workaround or patch available at time of publishing. Vulnerability may be exploited using a web client; however, a Proof of Concept exploit has been published.	SPiD File Include	Not available	Security Focus, Bugtraq ID: 16822, February 25, 2006
SquirrelMail Development Team SquirrelMail 1.4.5 & prior	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'webmail.php' due to insufficient sanitization of the 'right_main' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of input passed to comments in styles before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the	SquirrelMail Multiple Cross-Site Scripting & IMAP Injection CVE-2006-0188 CVE-2006-0195 CVE-2006-0377	**2.3** (CVE-2006-0188) **2.3** (CVE-2006-0195) **2.3** (CVE-2006-0377)	Secunia Advisory: SA18985, February 22, 2006 **Mandriva Linux Security Advisory, MDKSA-2006:049, February 27, 2006**

	'sqimap_mailbox_select mailbox' parameter due to insufficient sanitization before using in an IMAP query, which could let a remote malicious user inject arbitrary IMAP commands. The vulnerabilities have been fixed in the CVS repository and fixes will be included in the upcoming 1.4.6 version. **Mandriva** There is no exploit code required.			
Thomson SpeedTouch firmware 5.3.2.6.0	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the 'LocalNetwork' page due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because remote malicious users can create users that cannot be deleted via scripting code in the '31' parameter in a 'NewUser' function. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through use of a web client; however, a Proof of Concept exploit has been published.	Thomson SpeedTouch 500 Series Cross-Site Scripting CVE-2006-0946 CVE-2006-0947	2.3 (CVE-2006-0946) 7 (CVE-2006-09467	Security Focus, Bugtraq ID: 16839, February 25, 2006
WEB Insta Limbo CMS 1.0.4 .2	An HTML injection vulnerability has been reported due to insufficient sanitization of the message field in the Contact Form, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited using a web client.	WEBInsta Limbo HTML Injection CVE-2006-0934	2.3	Security Focus, Bugtraq ID: 16811, February 24, 2006
Woltlab Burning Board 2.7, 2.6, 2.5, 2.4, 2.3.3, 2.3.1, 2.2.2, 2.0 RC1 &RC2, 2.0 beta 3-beta5, 1.1.1	Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through use of a web client; however, a Proof of Concept exploit has been published.	Woltlab Burning Board Multiple Cross-Site Scripting	Not available	Security Focus, Bugtraq ID: 16843, February 27, 2006
WordPress WordPress 2.0.1.	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'wp-comments-post.php' due to insufficient sanitization of the 'Name' and 'Website' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because it is possible to disclose the full path to certain scripts by accessing them directly. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	WordPress Cross-Site Scripting & Path Disclosure	Not available	Secunia Advisory: SA19050, March 1, 2006
ZoneO Software freeForum 1.2	Several vulnerabilities have been reported: a vulnerability was reported in 'func.inc.php' due to insufficient sanitization of the 'X-Forwarded-For' and 'Client-Ip' HTTP headers before saving, which could let a remote malicious user execute arbitrary PHP code; and a Cross-Site Scripting vulnerability was reported in 'func.inc.php' due to insufficient sanitization of the 'name' and 'subject' parameters before saving, which could let a remote malicious user execute arbitrary HTML and script code.	freeForum Arbitrary PHP Code Execution & Cross-Site Scripting	Not available	Secunia Advisory: SA19020, February 28, 2006

	Update available Vulnerabilities can be exploited through use of a web client.

[back to top]

Wireless Trends & Vulnerabilities

This section contains wireless vulnerabilities, articles, and malicious code that has been identified during the current reporting period.

- Trojan targets basic Java phones: According to Kaspersky Labs, a Trojan has been created that can infect mobiles phones running Java applications. RedBrowser-A infects smart phones but can also infect any mobile phone capable of running Java (J2ME) applications. The mobile malware poses as a program that supposedly allows surfers to visit WAP sites without using a WAP connection.
- New virus closes PC/Windows Mobile gap: The Mobile Antivirus Researchers Association claims to have detected the first worm that can jump from a PC to a Windows Mobile-powered wireless device. The 'Crossover' worm nests itself in a directory on a Windows PC where it will automatically activate once the user connects a Windows Mobile device using Microsoft ActiveSync. This is a a Proof of Concept designed to show off its features but not cause any actual harm.
- Is your cell phone due for an antivirus shot? Programs that fight viruses have become a necessary evil on Windows PCs but now the antivirus industry is turning its attention to mobile phones. However it is running into reluctance from cell service providers, who aren't so sure that the handset is the best place to handle security.

[back to top]

General Trends

This section contains brief summaries and links to articles which discuss or present information pertinent to the cyber security community.

- Kits help phishing sites proliferate: According to the Anti-Phishing Working Group's report for December, the number of phishing e-mails fell between November and December last year, and the number of fraudulent Web sites increased from 4,630 to 7,197, which is a record. Security companies believe the increasing number of phishing Web sites can be attributed to the easy availability of phishing kits, tools that can be used by relatively nontechnical people to create and manage multiple phishing sites. According to Internet security company Websense, one of the most popular phishing kits is called Rock Phish Kit, which the company said was first seen last November.
- Politically motivated attacks soar in 2005: According to an independent report, web server attacks and website defacements rose 16 per cent last year. Zone-h, the security firm best known for its defacement archive, recorded 495,000 web attacks globally in 2004, up from 393,000 in 2003. The largest category in 2005 was mass defacements (371,000). More targeted attacks on individual servers numbered 124,000. There was also an increase in politically motivated attacks. A growing number of these attacks were launched from Muslim countries, especially Turkey; however, the majority of attacks launched in 2004 originated in Brazil. The most active defacer last year was Iskorpitx, from Turkey, who's bagged 90,000 websites over the last two years.
- Keyloggers on the rise: Keylogging use for illegal activity is continuing to rise. The New York Times has an article discussing the growing trend of keyloggers used by criminals to steal banking information from unwary users. As the news coverage of keyloggers becomes more mainstream, the magnitude of the growing problem becomes more apparent.
- 'Phishing' Season For Tax Scammers: According to Government officials, they are currently seeing one widespread IRS-themed e-mail scam a week. Internet security experts expect this to escalate as the April 15 deadline nears. E-mails that appear to be from the Internal Revenue Service are really identity theft scams designed to collect personal financial information.
- Malware moves up, goes commercial: While in the process of researching a new trojan, engineers at Panda Software uncovered evidence that led them to a web site selling custom-built viruses. For a price of only $990 (U.S.), a user gets his or her own trojan horse. This comes complete with tech support. If the file is discovered, the designer provides a guarantee to alter it so that it may continue to avoid detection in the face of updated antivirus software.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folder.
2	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.

3	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender's address.
4	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
5	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
6	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
7	Sober-Z	Win32 Worm	Stable	December 2005	This worm travels as an email attachment, forging the senders address, harvesting addresses from infected machines, and using its own mail engine. It further download code from the internet, installs into the registry, and reduces overall system security.
8	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
9	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
10	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.

Table updated February 28, 2006

[back to top]

Last updated March 02, 2006